



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

09/834,106

04/13/2001

Bao Feng

45539-20009.00

5315

25227

7590

06/02/2006

MORRISON & FOERSTER LLP  
1650 TYSONS BOULEVARD  
SUITE 300  
MCLEAN, VA 22102

EXAMINER

PARTHASARATHY, PRAMILA

ART UNIT

PAPER NUMBER

2136

DATE MAILED: 06/02/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

# Office Action Summary

Application No.

09/834,106

Applicant(s)

FENG ET AL.

Examiner

Pramila Parthasarathy

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

## Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

- 1) ☒ Responsive to communication(s) filed on 18 April 2006.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

- 4) ☒ Claim(s) 1-32 is/are pending in the application.
- 4a) Of the above claim(s) 1-8 is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 9-32 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

## Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some \* c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

## Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_.
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_.

## **DETAILED ACTION**

### ***Continued Examination Under 37 CFR 1.114***

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114.

2. Applicant's submission filed on April 18, 2006 has been entered and made of record.

### ***Claim Rejections - 35 USC § 112***

3. Applicant's amendments with respect to Claims 9 – 32 have been fully considered and are persuasive. The rejection 35 USC 112 of Claims 1 – 41 has been withdrawn. However, upon further consideration, the amended Claims 9 – 32 have been rejected under 35 USC 112.

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

4. Claims 9 – 32 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

The amended independent Claims 9, 13, 17, 21, 25 and 29 read, “ ... a first cryptography scheme;” and “a second cryptography scheme;”.

With respect to “cryptography scheme”, although the specification discloses the digital objects are encrypted with a symmetric key cryptosystem, the specification does not disclose a first cryptography scheme and a second cryptography scheme. The specification does not indicate what these first or second cryptography schemes and how they are used to encrypt the plurality of encryption keys. Applicant amendment does not clarify the steps of encrypting the plurality of encryption keys using a first cryptography scheme or encryption key has been further encrypted using a second cryptography scheme.

The dependent claims 10 – 12, 14 – 16, 18 – 20, 22 – 24, 26 – 28 and 30 – 32 are rejected at least by virtue of their dependency on the dependent claims.

***Response to Arguments***

5. Regarding currently amended claims 9 – 32, Applicant argues that the prior art Gammie et al. (U.S. Patent Number 5,237,610) fails to disclose the claimed invention and do not teach, “enables a user to securely request content from a database while obscuring from the database operator what content was of primary interest to the requester”. This argument is not found persuasive. Applicant has not claimed “a user to securely request content from a database while obscuring from the database operator what content was of primary interest to the requester”.

Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references.

Applicant agrees with the Examiner that Gammie discloses the twice-encrypted content is received at a receiver where it is twice-decrypted and that the pending claims describe that a once-encrypted key is transmitted from a database to a requester. The examiner respectfully asserts that the cited prior art does teach or suggest the amended subject matter “a once-encrypted key is transmitted from a database to a requester” broadly recited in the amended independent claims (Column 19 line 59 – Column 20 line 28). The dependent claims 10 – 12, 14 – 16, 18 – 20, 22 – 24, 26 – 28 and 30 – 32

are rejected at least by virtue of their dependency on the dependent claims and by other reason set forth in this office action. Accordingly, the rejection for the pending claims 9 – 32 is respectfully maintained.

Examiner suggests applicant to amend the claims in a manner to distinct applicant's invention with prior art with **attention** given to the instant application specification paragraphs [0029 – 0035].

### ***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claims 9 – 32 are rejected under 35 U.S.C. 102(b) as being anticipated by Gammie (U.S. Patent Number 5,029,207).

7. Regarding Claims 9, 17 and 25 Gammie

discloses generating a plurality of encryption keys, each encryption key associated with one of a plurality of digital objects stored in an electronic database (Summary and Column 9 line 65 – Column 10 line 13);

encrypting the plurality of digital objects using the associated encryption keys  
(Summary and Column 9 line 65 – Column 10 line 15);

encrypting the plurality of encryption keys using a first cryptography scheme  
(Summary and Column 9 line 65 – Column 10 line 15);

transmitting to a requester the plurality of encrypted digital object and encryption  
keys (Summary and Column 9 line 65 – Column 10 line 13);

receiving from the requester at least one of the encryption keys, wherein the  
received encryption key has been further encrypted using a second cryptography  
scheme (Summary and Column 9 line 65 – Column 10 line 20);

generating a partially decrypted encryption key by decrypting the received  
encryption key using the first cryptography scheme (Summary and Column 9 line 65 –  
Column 10 line 29); and

transmitting the partially decrypted encryption key to the requester (Summary  
and Column 9 line 65 – Column 10 line 37).

8. Regarding Claims 13, 21 and 29 Gammie discloses requesting a plurality of  
digital objects from an electronic database (Summary and Column 12 lines 21 – 36);

receiving from the database the requested plurality of digital objects, wherein  
each digital object has been encrypted using an associated encryption key (Summary  
and Column 12 lines 21 – 36);

receiving from the database plurality of keys associated with the plurality of digital objects wherein each key has been encrypted using a first cryptography scheme (Summary and Column 12 lines 21 – 36);

selecting a key from the plurality of received keys (Summary and Column 12 lines 21 – 36);

further encrypting the selected key using a second cryptography scheme (Summary and Column 12 lines 21 – 36);

transmitting the key to the database (Summary and Column 12 lines 21 – 36);

receiving from the database the key wherein the key has been partially decrypted using the first cryptography scheme (Summary and Column 12 lines 21 – 36);

decrypting the partially decrypted key using the second cryptography scheme to generate a decrypted key (Summary and Column 12 lines 21 – 36); and

decrypting the received digital object using the decrypted key (Summary and Column 12 lines 21 – 36).

9. Claims 10, 14, 18, 22, 26 and 30 are rejected as applied above in rejecting Claims 9, 13, 17, 21, 25 and 29. Furthermore, Gammie teaches encrypting the plurality of encryption keys by determining  $(\text{encryption key})^{(\text{random number } R)} \bmod (\text{prime number } p)$  for each key (Column 2 lines 14 – 28).

10. Claims 11, 15, 19, 23, 27 and 31 are rejected as applied above in rejecting Claims 9, 13, 17, 21, 25 and 29. Furthermore, Gammie teaches decrypting the received



encryption key by determining  $(\text{encryption key})^{(1/(\text{random number } R) \bmod (\text{prime number } p-1))} \bmod$   
(prime number  $p$ ) (Column 2 lines 14 – 28).

11. Claims 12, 16, 20, 24, 28 and 32 are rejected as applied above in rejecting Claims 10, 14, 18, 22, 26 and 27. Furthermore, Gammie teaches performing the modulo operation if computation of a discrete logarithm is not possible (Column 2 lines 14 – 28).

### ***Conclusion***

Examiner's Note: Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant.

Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant, in preparing the responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.


The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO Form 892.

Applicant is urged to consider the references. However, the references should be evaluated by what they suggest to one versed in the art, rather than by their specific disclosure. If applicants are aware of any better prior art than those are cited, they are required to bring the prior art to the attention of the examiner.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 571-272-3866. The examiner can normally be reached on 8:00a.m. To 5:00p.m.. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-232-3795. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR only. For more information about the PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Pramila Parthasarathy  
May 29, 2006.

  
AYAZ SHEIKH  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100